Cybersécurité en santé

Ce Programme a bénéficié d'une aide de l'État gérée par l'Agence Nationale de la Recherche au titre de France 2030 portant la référence xANR_22-CMAS-0014 3.951.200

SOMMAIRE

1. Introduction

SaNuRN
Santé Numérique Rouen Nice

1. a. Objectifs pédagogiques

› Comprendre les enjeux de la cybersécurité / risques cyber

› Concevoir et maintenir sécurisé son environnement numérique de travail (personnel ET professionnel)

› Connaître les risques potentiels les plus courants et/ou les plus probables

› Se prémunir et réagir face aux incidents

1. b. Définition de la cybersécurité (en santé)

› Connaître les risques potentiels les plus courants et/ou les plus probables. La cybersécurité en santé englobe un ensemble de **pratiques**, de **politiques** et de **technologies** visant à protéger les données médicales sensibles et les systèmes d'information dans le secteur de la santé. Cela inclut la prévention des accès non autorisés, la confidentialité et la disponibilité des données.

› La cybersécurité s'inscrit dans la souveraineté d'un territoire et plus généralement d'un État. Sa mise en place est donc, le plus souvent, l'affaire du pays, du moins dans sa politique globale.

› Il s'agit de protéger l'intégrité, la disponibilité et la confidentialité des données sensibles, mais aussi de prévenir les risques d'usurpation d'identité et d'extorsion financière.

2. Importance de la cybersécurité

SaNuRN
Santé Numérique Rouen Nice

2. a. Son importance aujourd'hui

› Les systèmes de santé dépendent des technologies de l'information pour stocker et gérer les données médicales.

› La cybersécurité en santé est cruciale pour garantir la confiance des patients, maintenir la qualité des soins et éviter les conséquences graves des violations de données.

2. b. Quelques chiffres*

Entre 2021 et mars 2023 : 215 incidents recensés en santé

dont 42% à l'hôpital

50 000€ c'est le coût médian d'une cyberattaque

47 % des télétravailleurs se font piéger par un *phishing*

*sources : https://www.paymed.pro, https://www.stoik.io, juin 2023

3. Les données en santé

SaNuRN
Santé Numérique Rouen Nice

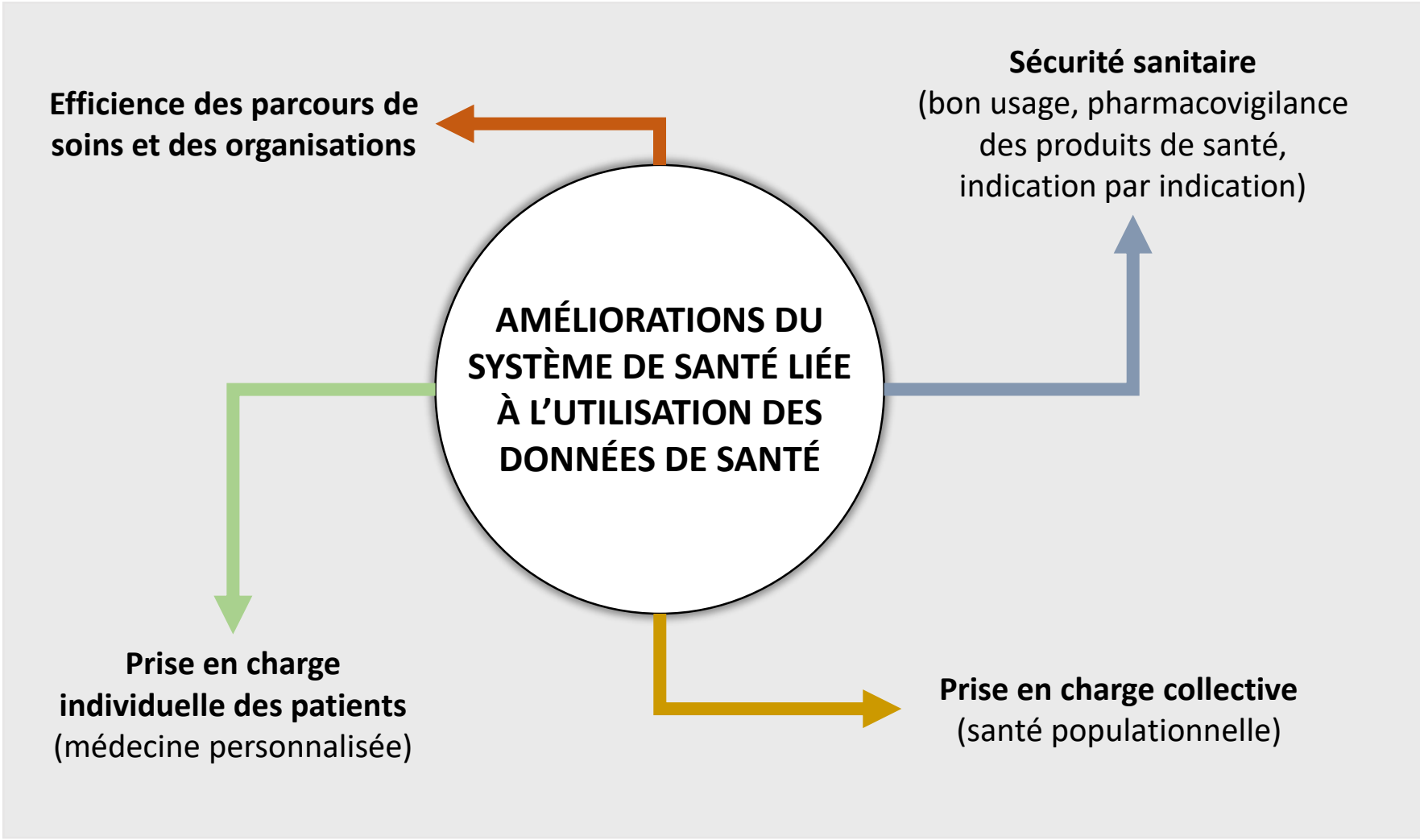
3. a. Qu'est-ce qu'une donnée de santé ?

- Données qui sont « par nature » relatives à l'état de santé d'une personne (celles issues de la relation de soin par exemple)

- Mais aussi les constantes physiologiques et caractéristiques morphométriques de l'homme sain (définition de la santé !)

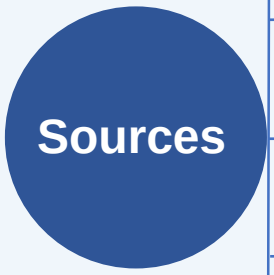
- Données qui le seraient compte tenu de leur destination (telles que celles issues de certains objets connectés, avec différents niveaux de granularité : exemple des trains de glycémies répétées).

3. b. Enjeux des usages de la donnée



3. c. Sources des données en santé

One Digital Health



- **DOSSIER MÉDICAL**
  Etablissements de santé/professionnels de ville
- **ESSAIS CLINIQUES**
  (privés/publics)
- **BASES DE DONNÉES**
  Médico-Administratives SNIIRAM* : 8,9 milliards de feuilles de soins en 2015, 20 milliards en lignes, PMSI**
- **DONNÉES DES PATIENTS**
  Objets connectés, applications
- **COHORTES/REGISTRES**
  Constances (200 000 volontaires de 18 à 69 ans), Hepater
- **DONNÉES D'OPINION**
  Réseaux sociaux, sites internet, moteurs de recherche
- **DONNÉES OMIQUES**
  Génomique, transcriptomique, protéomique, métabolomique (voir schéma)
- **DONNÉES ENVIRONNEMENTALES**
  Exposome
- **DONNÉES SANTÉ VÉTÉRINAIRE**

SNIIRAM* : Système national d'information inter-régimes de l'assurance maladie
PMSI** : Programme de médicalisation des systèmes d'information

4. Les référentiels de cybersécurité

SaNuRN
Santé Numérique Rouen Nice

4. a. PGSSI

La Politique Générale de Sécurité des Systèmes d'Information de Santé encadre les règles de sécurité pour l'e-santé.

4. b. ANSSI

L'Agence Nationale de la Sécurité des Systèmes d'Information propose un Guide d'hygiène informatique afin de renforcer la sécurité de son système d'information.

4. c. RGPD

Le Règlement Général sur la Protection des Données de l'UE s'applique à toutes les données personnelles, y compris celles dans le secteur de la santé. Il impose des obligations strictes de protection des données et de notification en cas de violation.

4. d. Norme HDS

➢ *Norme française régissant le stockage et la gestion des données de santé*

1. **Sécurité renforcée**
   - Les hébergeurs de données de santé doivent respecter des exigences strictes en matière de sécurité, notamment en termes de cryptage, de contrôles d'accès, de surveillance, et de gestion des risques. Ces mesures garantissent une protection accrue des données sensibles.

2. **Confidentialité**
   - La norme HDS impose des règles strictes pour garantir la confidentialité des données de santé. Les hébergeurs doivent mettre en place des mesures spécifiques pour empêcher l'accès non autorisé aux informations médicales.

3. **Intégrité des données**
   - La norme HDS exige des mécanismes pour garantir que les données de santé ne sont ni altérées ni perdues, assurant ainsi l'intégrité des informations.

4. **Gestion des accès**
   - Les hébergeurs de données de santé doivent mettre en place des systèmes de contrôle d'accès qui permettent uniquement aux personnes autorisées d'accéder aux données médicales, tout en maintenant des journaux d'audit pour suivre les activités.

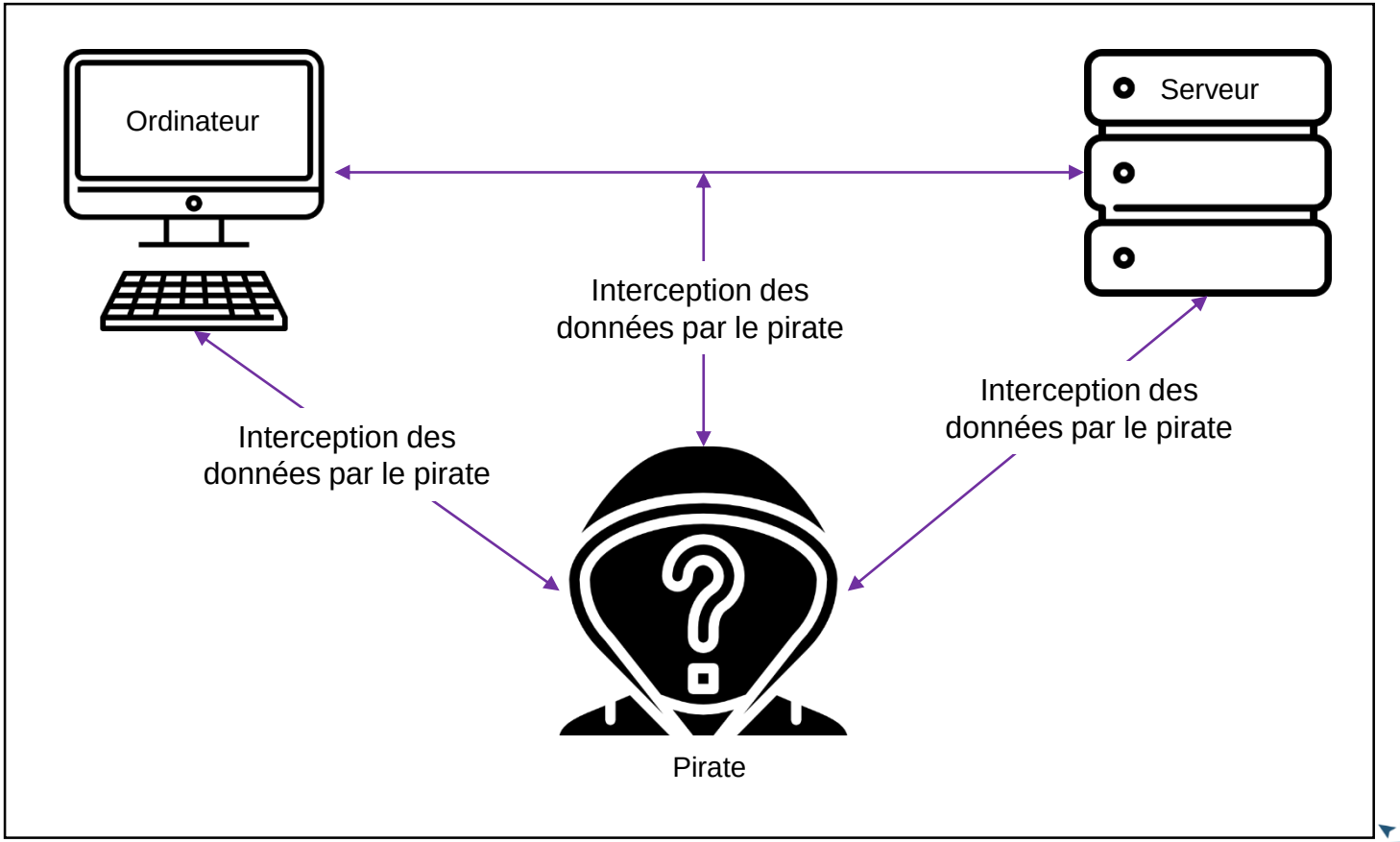
5. **Certification**
   - Les hébergeurs de données de santé doivent obtenir une certification HDS délivrée par une autorité de santé compétente. Cette certification atteste de leur conformité aux normes et réglementations en vigueur.

5. Les menaces courantes

SaNuRN
Santé Numérique Rouen Nice

5. a. Les principales menaces

- Virus
- Logiciels malveillants
- Phishing (hammeçonnages)
- Ransomwares



5. a. Les principales menaces : définitions

- **Un virus informatique** est un automate autoréplicatif à la base non malveillant, mais aujourd'hui souvent additionné de code malveillant (donc classifié comme logiciel malveillant), conçu pour se propager à d'autres ordinateurs

- **L'hameçonnage** (ou *phishing* en anglais*)* est une technique utilisée par des fraudeurs pour obtenir des renseignements personnels dans le but de perpétrer une usurpation d'identité. La technique consiste à faire croire à la victime qu'elle s'adresse à un tiers de confiance — banque, administration, etc. — afin de lui soutirer des renseignements personnels : mot de passe, numéro de carte de crédit, numéro ou photocopie de la carte d'identité, date de naissance, etc.

5. a. Les principales menaces : définitions

- **Un rançongiciel** (*ransomware*) (=logiciel rançonneur, logiciel de rançon ou logiciel d'extorsion), est un logiciel malveillant qui « prend en otage » des données personnelles. Pour ce faire, un rançongiciel chiffre des données personnelles puis demande à leur propriétaire d'envoyer de l'argent en échange de la clé qui permettra de les déchiffrer. Au-delà de la confiscation de la donnée, cela peut paralyser un système d'information et donc une activité entière.

- **Attaque par déni de service distribué** (DDoS) : attaque ciblée par un grand nombre d'ordinateurs sur un serveur ou site particulier avec un afflux conséquent de requêtes simultanées

- ***Le vol de données n'est pas systématique***

5. a. Les principales menaces : qui ?

- Les attaques sont menées par des pirates informatiques, parfois organisés en groupes, voire par des organisations criminelles nationales ou internationales. Les experts estiment que la cybercriminalité est en train de se structurer en une véritable industrie.

- Des équipes spécialisées sont structurées pour lutter contre ces groupes et individus.

- Jeu du « chat et de la souris » permanent

5. b. Exemples de cyberattaques

Les établissements de santé sont particulièrement visés par les cyberattaques :

- En 2019, le CHU de Rouen a été victime d'un *ransomware*, ce qui conduit à un arrêt total du système informatique de l'hôpital.
- En 2022, des pirates ont attaqué le réseau du GHT Cœur Grand Est exigeant une rançon de 1,3 million de dollars, puis ont vendus ces données sensibles sur le darknet.

Les administrations publiques, tout aussi vulnérables :

- En 2022, le Conseil départemental de la Seine-Maritime a été victime d'une cyberattaque majeure, provoquant une paralysie des services, des réseaux coupés, et un impact significatif sur les usagers, avec des conséquences durables pour l'administration publique du département.

5. c. Retours

Exemple CHU de Rouen : en 2023, environ 18 000 attaques par jour !

› Lors de la paralysie d'un Système d'Information Hospitalier, les systèmes « clés » à réactiver en priorité sont :
- Logiciel de gestion de la stérilisation (chirurgie)
- Gestion des blocs chirurgicaux
- Service des urgences
- Dossier Patient Informatisé
- PACS (imagerie)
- Facturation/Paie
- ...

› Difficultés pour savoir :
- si des données ont été volées
- si les systèmes sont à nouveau « sains » (vierges de toutes menaces)

› Coûts élevés pour remettre les systèmes en fonctionnement, impact important sur les budgets...

6. Violation des données personnelles

SaNuRN
Santé Numérique Rouen Nice

6. a. Définition de la violation des données personnelles selon le RGPD

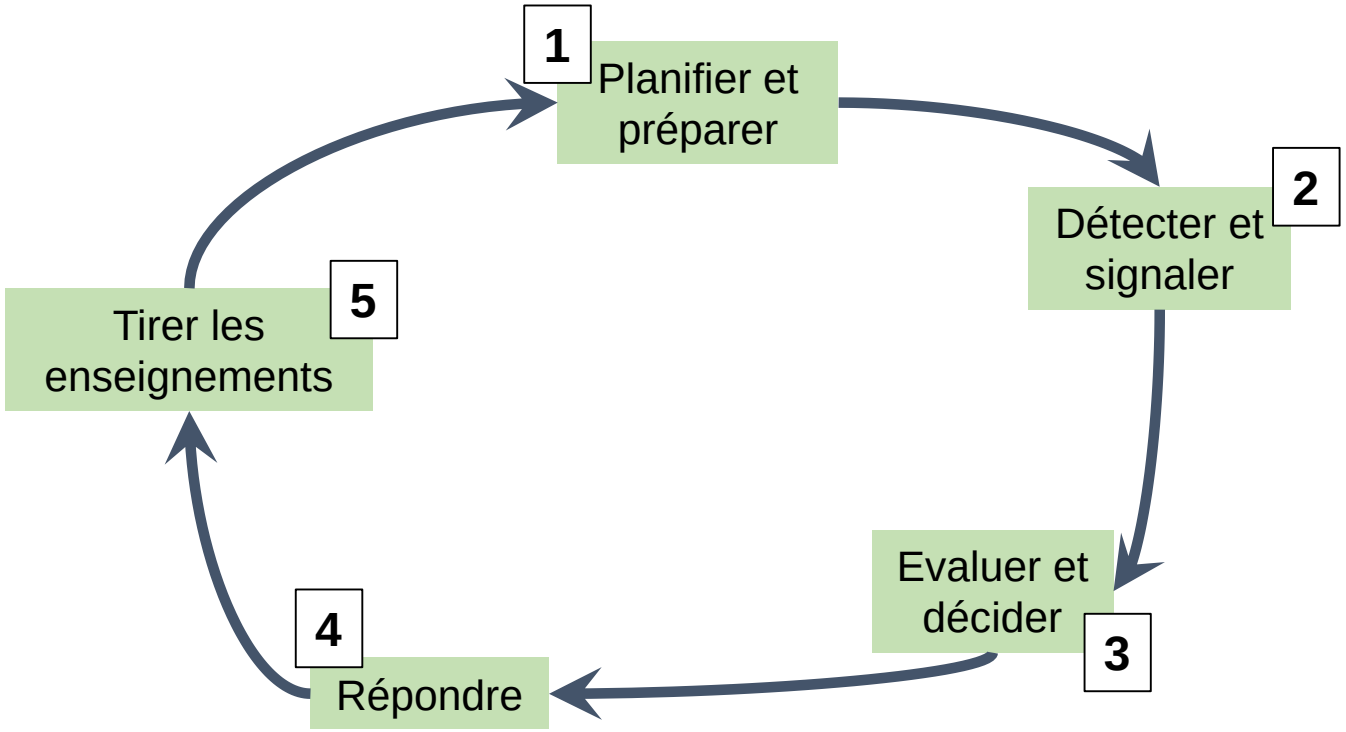
*« Une violation de la sécurité se caractérise par la **destruction**, la **perte**, l'**altération**, la **divulgation** non autorisée de données à caractère personnel transmises, conservées ou traitées d'une autre manière, ou l'**accès non autorisé** à de telles données, de manière accidentelle ou illicite. »* selon le CNIL.

Par exemple :

- Vol ou perte d'une clé USB contenant des données sensibles.
- Publication en ligne ou vente d'informations personnelles sans le consentement de l'individu
- Consultation de dossiers médicaux non autorisé

6. b. Procédures d'identification et signalement

Processus de Gestion des incidents



7. Réagir aux incidents

SaNuRN
Santé Numérique Rouen Nice

7. a. Plan de réponse aux incidents et actions

Préparation :

- Établissement d'une équipe de réponse aux incidents (CSIRT - Computer Security Incident Response Team) comprenant des experts en sécurité informatique.
- Développement d'un plan de réponse aux incidents décrivant les rôles et responsabilités de chaque membre de l'équipe.
- Identification des actifs critiques et des vulnérabilités dans le système d'information.
- Mise en place de mécanismes de surveillance pour détecter les incidents de sécurité.

7. a. Plan de réponse aux incidents et actions

Détection :

- Surveiller en permanence le réseau et les systèmes pour détecter des activités suspectes ou des indicateurs de compromission (IOCs).
- Analyser les journaux (logs) et les alertes générées par les systèmes de sécurité pour identifier les signes d'une éventuelle cyberattaque.

Containment (Contenir) :

- Isoler les systèmes compromis ou vulnérables pour empêcher la propagation de l'attaque.
- Identifier et mettre hors service les vecteurs d'attaque.
- Recueillir des preuves et des informations sur l'incident.

7. a. Plan de réponse aux incidents et actions

Éradication :

- Éliminer complètement la menace en supprimant les logiciels malveillants, en corrigeant les vulnérabilités et en rétablissant l'intégrité des systèmes.
- Mettre à jour les systèmes et les logiciels pour éviter de futures attaques similaires.

Recovery (Rétablissement) :

- Restaurer les services et les données affectés tout en surveillant leur intégrité.
- Rétablir la confiance des utilisateurs et des clients.

7. a. Plan de réponse aux incidents et actions

Communication :

- Informer les parties prenantes internes et externes, y compris la direction, les clients, les autorités et les médias, conformément aux lois et réglementations en vigueur.
- Fournir des mises à jour régulières sur la situation et les progrès de la réponse à l'incident.

Analyse post-incident :

- Examiner l'incident pour comprendre comment il s'est produit et comment il aurait pu être évité.
- Mettre en place des mesures correctives pour renforcer la sécurité du système.

Amélioration continue :

- Utiliser les enseignements tirés de l'incident pour améliorer les politiques, les procédures et les mécanismes de sécurité.

8. Hygiène numérique

SaNuRN
Santé Numérique Rouen Nice

8. a. Mesures collectives

› **Sauvegarder** les données critiques contenant des informations confidentielles en étant hors ligne pour minimiser les risques de fuite ;

› **Suivre des programmes de sensibilisation** et de formations pour ses pratiques de sécurité ;

› **Analyser** régulièrement les vulnérabilités ;

› **Effectuer** régulièrement des mises à jour des logiciels et des systèmes d'exploitation ;

› **Suivre les bonnes pratiques** d'authentification lors d'un accès à distance (bastion) ;

› **Mettre en place des exercices** de crise pour s'assurer de la continuité des soins ne serait pas affectée en cas d'attaque ;

› Pour les directions, **s'engager pleinement** sur la thématique de la cybersécurité, ce qui est rendu obligatoire par la directive Network and Information Security 2.

8. b. Mesures individuelles (hygiène numérique)

› **Se sensibiliser** régulièrement et sensibiliser son entourage (personnel et professionnel)

› **Connaître** son environnement informatique (pas dans le détail)

› **Authentification** :

Gestion des mots de passe

- règles de base (nombre de caractères, caractères spéciaux)
- changer *régulièrement*
- de pas utiliser le même mot de passe partout
- utiliser un « coffre-fort numérique »

› utilisation des cartes de santé

› **Bien choisir** les solutions informatiques (boites mail, etc.)

› Sur les dispositifs personnels :

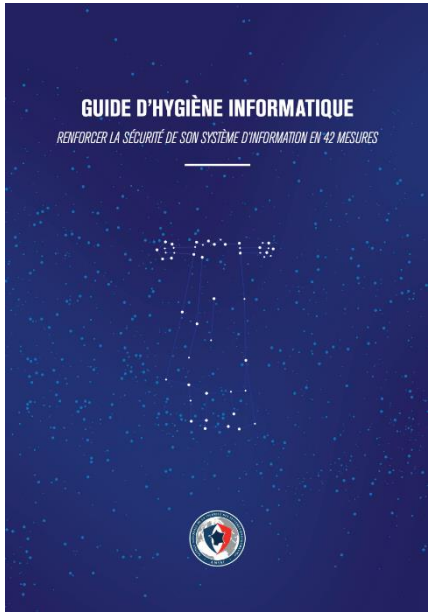
- **mettre à jour** régulièrement les systèmes
- attention à **bien supprimer/nettoyer les données** quand on se sépare d'un dispositif

9. Conclusion

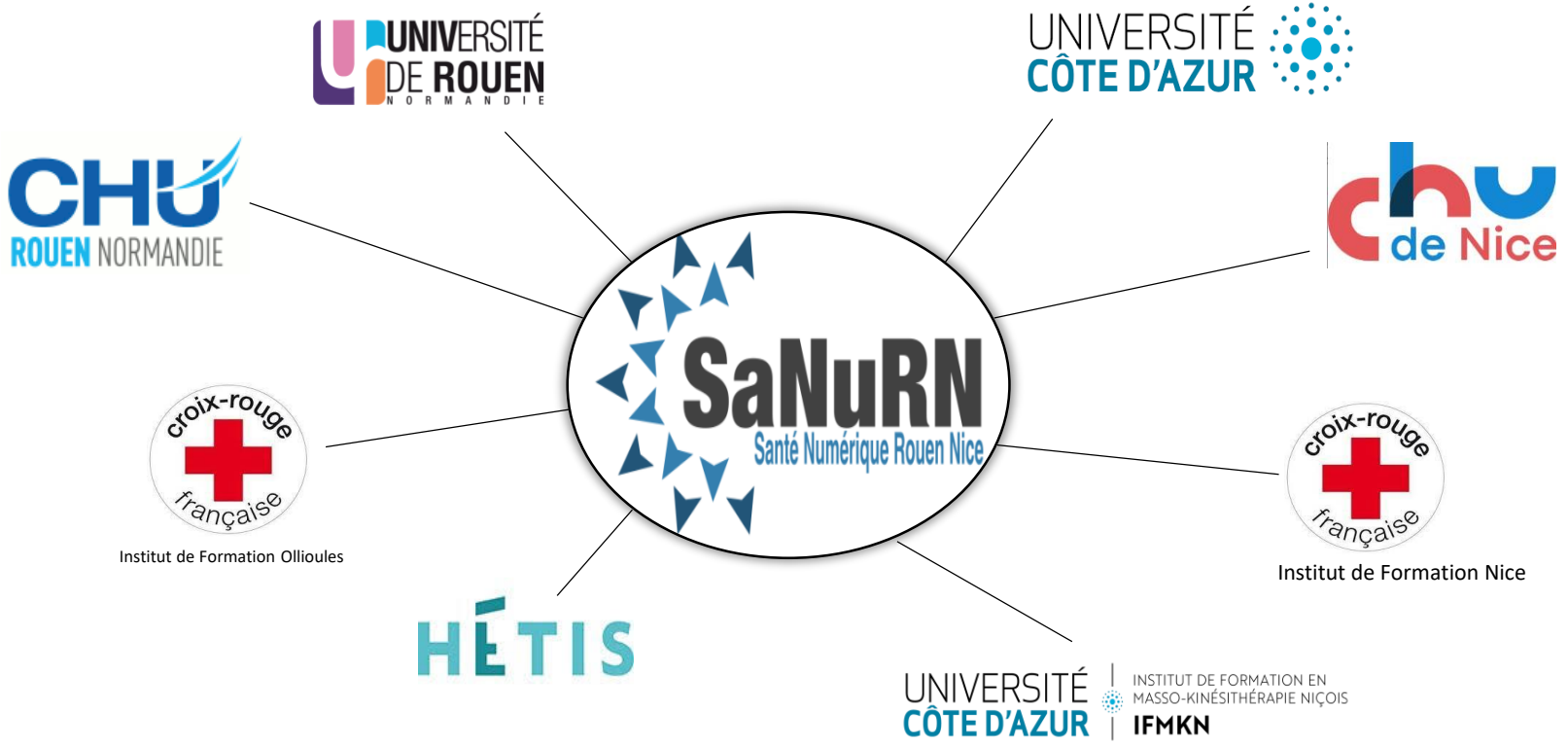
SaNuRN
Santé Numérique Rouen Nice

9. a. Résumé des points clés

- **La cybersécurité est l'affaire de toutes et tous** même si les spécialistes sont là pour conseiller et mettre en place des campagnes de prévention
- **Les attaques et incidents sont de plus en plus nombreux**, notamment dans le secteur de la santé
- Ce secteur est particulièrement **sensible** et fait l'objet de **réglementations** particulières (HDS...)
- Le **risque zéro n'existe pas** mais il faut apprendre de ses erreurs
- Une bonne « **hygiène numérique** » est essentielle !



UN PROJET MULTI-PARTENARIAL



RÉPUBLIQUE FRANÇAISE
anr agence nationale de la recherche
Ce Programme a bénéficié d'une aide de l'État gérée par l'Agence Nationale de la Recherche au titre de France 2030 portant la référence xANR_22-CMAS-0014 3.951.200
FRANCE 2030